

---

Records Management Program – Policies & Procedures

If yes, please provide a copy of the inventory.

10. Do you have records/information stored off-site?

- a. Yes
- b. No

11. If yes, do you have a contract with an off-site storage vendor?

- a. Yes
- b. No

If yes, please provide a copy of the contract and the company contact.

12. Does your department use the LAN to store records/information?

- a. Yes
- b. No

13. Does your department use the LAN to share records/information with other groups?

- a. Yes
- b. No

14. Does the department purge records/information from the LAN?

- a. Yes
- b. No

15. Does the department use or own any other servers (i.e., web, mid-range, etc.)?

- a. Yes.
- b. No

If yes, what?

16. Does the department back-up its computers?

- a. Yes
- b. No

17. Does the department have laptops, desktops or both?

- a. Laptops
- b. Desktops
- c. Both

18. Are employees required to take the laptops home or secure them in the office?

- a. Take Home
- b. Lock Up
- c. Either
- d. Neither required

19. What percentage of on-site records are inactive (used less than once a month)?

Records Management Program – Policies & Procedures

---

20. Are your records originals or copies?
- Originals
  - Copies
  - Both
21. What percentage are originals?
22. Does the department generate the originals or are they sent to you by others?
- Generate originals
  - Sent by others
  - Both
23. Does the department generate the copies it maintains or are they sent to you by others?
- Generate copies
  - Sent by other departments
  - Both
24. Do you have a central filing area or file cabinets throughout the department?
- Central filing area
  - Cabinets throughout
  - Neither
  - Both
25. Are files retained in employee's offices or cubes?
- Yes
  - No
26. Is your floor or area accessible by anyone during work hours?
- Yes
  - No
27. Do you know where your system back-ups are being stored?
- Yes
  - No
- If yes, where?
28. Who, within your department, is responsible for retaining records on-site and/or storing records off-site? Please provide name(s) and telephone number(s).

MCIWC031889

## APPENDIX L

### Compliance Audit Exhibits

## APPENDIX M

### RRI

#### List of HLQs and Required Retention

MCIWC031891

## APPENDIX N

LPP's

“E-Mail Guidelines”

Records Management Program – Policies & Procedures

---

-----Original Message-----

**From:** O'Neil, Thomas F.  
**Sent:** Sunday, October 31, 1999 10:12 PM  
**Subject:** E-Mail Guidelines

Attached are E-Mail Guidelines which we have drafted to address various legal risks created by the Company's extensive use of e-mail as a preferred mode of communication. The Guidelines include various practical suggestions about drafting and retaining e-mail messages. I would very much appreciate your forwarding electronic or hard copies of this document to all appropriate personnel in your respective organizations. Feel free to call me if questions arise as folks review it.

Thanks very much.

Tom O'Neil  
Chief Litigation Counsel

**E-Mail Guidelines<sup>1</sup>**

**Thomas F. O'Neil III**

Chief Litigation Counsel  
MCI, Inc.

Based in large part on lessons learned from extensive internal review of records in connection with civil litigation and enforcement proceedings, we have drafted the following Guidelines concerning the use, content and retention of electronic mail ("e-mail"). Virtually all MCI, Inc. ("MCI" or the "Company") employees now rely heavily on e-mail as the primary mode of business-related communication and, for the reasons set forth below, it is critical that you use it carefully.

Many people treat e-mail exchanges casually--indeed cavalierly--as if they are equivalent to a private telephone conversation. This approach can subsequently jeopardize the Company's interests in a way that typically is never envisioned when the message is drafted. That is because unlike a telephone conversation that ends when the call is terminated, an e-mail message is a written communication that creates a record, which can easily be forwarded, printed, and stored electronically, and which often cannot be truly deleted or discarded by the author or the recipient. Like other written materials, individuals, entities and regulatory officials can obtain our e-mail through discovery mechanisms in civil and enforcement proceedings. Accordingly, whenever you address a sensitive subject, such as technological or fiscal feasibility, or the ethical or legal permissibility of a new product, service or strategic proposal, you should consider using alternate means of communication, such as a meeting or a conference call. We hope these Guidelines will assist you in making that assessment.

---

MCIWC031893

## I. THE CONTENT OF E-MAIL MESSAGES

### A. Overview

#### **1. Internal Messages**

Although internal e-mail messages, by their very nature, tend to be less formal than external correspondence, you always should compose and transmit them with the understanding that they may well become public. If an e-mail would tend to confuse or embarrass you or the Company in a public forum, such as a deposition, a legislative hearing or a judicial proceeding, it should not be issued. This litmus test applies with equal force to the full gamut of messages, from highly personal musings to potentially troublesome reflections or admissions concerning pending business transactions. For this same reason, in drafting any e-mail message, you should not engage in unnecessary speculation about, for example, the motive's of a particular person or the outcome of a pending transaction.

Unintended disclosure of an internal e-mail message can occur in several ways. It might, for example, erroneously be sent to an inappropriate recipient as a result of the use of a wrong key – e.g., the “Reply All” function. At the same time, a recipient of an internal e-mail may forward it to an external party, naively trusting that recipient not to store or further transmit it. Finally, as previously noted, e-mail messages, unless covered by a recognized privilege, are subject to discovery in litigation, congressional investigations and regulatory enforcement proceedings.

#### **2. External E-Mail Messages**

As we all know, e-mail has virtually replaced hard-copy correspondence. Although e-mail messages are easier to compose and send than traditional letters, legally there is no distinction between them. Therefore, as with any written corporate communication, an external e-mail should express well-formulated and well-articulated thoughts. “Thinking out loud” is particularly inappropriate for such a message. In short, you should draft an external e-mail message with the same level of care and formality with which you would draft a business letter to the same recipient.

### B. Recommendations

With these content-based cautions in mind, we offer the following guidance. If a gratuitous comment could subsequently embarrass you, – for example, “Customer ‘X’ is sleazy;” “The regulators are crazy,” or “Let’s call Legal and say that we never understood the contract when we signed it,” do not type it. In the same vein, if you receive a message that evokes an emotional response on your part, be wary of answering by e-mail. At a minimum, wait until you are able to review it objectively for tone and content, and then reconsider the propriety of responding by way of e-mail.

We are all best-advised not to discuss via e-mail the question whether the Company, one of its subsidiaries, or one or more of its officers, directors, or employees has acted properly in certain circumstances. Never discuss or debate the legality of a situation through e-mail. It is equally unacceptable to suggest in e-

Records Management Program – Policies & Procedures

---

mail that legal advice be ignored. Finally, detailed discussions of sensitive strategic questions should never be pursued electronically.

## **II. PROPRIETARY OR PRIVILEGED INFORMATION**

### **A. Confidential/Proprietary E-mails**

Given the Company's preeminent position in a frenetic industry, it is inevitable that at some point you will need to resort to e-mail to transmit internally confidential or proprietary information, such as strategic planning documents, confidential customer information, and proprietary technical information. But before disseminating that type of information, you should consider the attendant "cyber-risks." If you decide to proceed, the message should include the following header: "CONFIDENTIAL INFORMATION – PLEASE DO NOT FORWARD, PRINT OR STORE ELECTRONICALLY." Because claims of confidentiality can be rendered vulnerable by overuse or misuse, this header should be used consistently and only when the e-mail actually contains confidential or proprietary information. When in doubt, please use the header.

### **B. Legal Privileges and E-mail**

Some e-mail messages may be covered by legal "privileges" that may protect them from disclosure. The most common of these is the attorney-client privilege.<sup>2</sup> Essentially, it applies to a confidential communication between a lawyer and a client (or the agent of either) for the purpose of obtaining legal advice. More specifically, in the corporate setting, the attorney-client privilege applies where (1) counsel is acting in a legal capacity, (2) the communication was understood to be confidential when made, and (3) the communication is disclosed only to essential corporate employees. The following maxims apply to privileged communications:

1. Use e-mail to disseminate privileged communications only when necessary. As noted, you should always try to avoid discussing via e-mail legal strategy, or to exchange privileged drafts of letters, contracts or pleadings. To the extent possible, messages seeking legal advice should not include unnecessary business discussions.

---

<sup>2</sup> For a detailed discussion of the attorney-client privilege, visit the LPP website at <https://teamnet2.mcilink.com/departments/lppgc/>



---

---

Records Management Program – Policies & Procedures

2. Merely “cc-ing” a lawyer on an e-mail message will not transform it into a privileged communication. It must satisfy the criteria of the test set forth above. To determine whether a communication truly is for the purpose of obtaining legal advice, a court will consider whether it is addressed directly, and primarily, to counsel and, even more importantly, whether the text of the message supports the claim of privilege.
3. Every privileged communication should be clearly marked “PRIVILEGED AND CONFIDENTIAL; SUBJECT TO THE ATTORNEY-CLIENT PRIVILEGE.” As with e-mail messages reflecting confidential or proprietary information, this header should be used consistently and after careful consideration of its applicability. Generally, you should use it whenever you send an e-mail message to an in-house lawyer seeking any sort of guidance.
4. Insofar as confidentiality is concerned, you should not disclose the contents of a privileged communication to anyone other than an employee of the Company who has a very real “need to know.” As noted above, copying or forwarding a privileged e-mail message to anyone else most likely will waive the privilege.
5. When possible, maintain all privileged communications in separate, clearly labeled files.

### III. DISTRIBUTION AND PRESERVATION OF E-MAIL MESSAGES

#### A. Broadcast E-Mails

E-mail enables an author to distribute a message to a broad audience in a matter of seconds. Although it may be critical in certain situations, such broad distribution of e-mail should not be the routine approach. Indeed, the Company has issued a Broadcast Messaging Policy requiring all such transmissions to be channeled through Corporate Employee Communications and subject to the approval of senior management.<sup>3</sup>

#### B. Forwarding E-Mail Messages

As a general rule, you should exercise great caution when forwarding comprehensive e-mail messages. In short, do so only when absolutely necessary. “Chain” or “nested” e-mail messages—i.e., those attaching a string of prior messages—present special concerns. Forwarding an otherwise privileged message to a non-lawyer or someone not employed by the Company typically will cause the protection afforded by the privilege to evaporate. Alternative approaches to consider here are drafting an entirely new message summarizing the key points, or “cutting and pasting” pieces of messages into a new, more succinct one.

---

<sup>3</sup> The Broadcast Messaging Policy can be found at [https://teamnet2.mcilink.com/departments/public\\_relations/messaging\\_policy/index.html](https://teamnet2.mcilink.com/departments/public_relations/messaging_policy/index.html).

C. Retention of E-Mail Messages

The Company has in place a mandatory records retention policy developed and monitored by our Records Management Department. This policy applies to all MCI entities and establishes retention criteria, which are generally based on the nature or content of a particular document. Because e-mail encompasses the full array of types of communications, the retention period is based on the content of the message in question. Thus, for example, an e-mail message between an MCI employee and a vendor must be retained for the time period specified for vendor correspondence.<sup>4</sup>

Unless otherwise covered by a specific retention requirement, internal e-mail need not be retained beyond its useful life unless it is relevant to ongoing litigation, an enforcement proceeding or an audit. Under such circumstances, you typically will be notified of the obligation to retain until further notice the pertinent hard copy and electronically stored materials.

\* \* \*

These Guidelines do not address every question that will arise in connection with e-mail usage. You should feel free, therefore, to call me (v222-6412/202-736-6412), Adam Charnes (v222-6093/202-736-6093) or Jamon Jarvis (v222-6342/202-736-6342) if you need more focused advice.

---

<sup>4</sup> For additional information regarding record retention policies, please consult the Records Management Department.

## APPENDIX O

### Training Presentations



Records and Information Management

---

# RECORDS COMPLIANCE PROGRAM

RIM's Website:

<https://teamnet2.mcilink.com/departments/rim/>

## MANDATORY PROGRAM

- ◆ The Company and its employees must adhere to all state, federal and operational record keeping requirements.
- ◆ All levels of management are held accountable for their department's compliance.
- ◆ Adherence to the Program and the requirements outlined in the Record Retention Schedule is mandatory, without exception.
- ◆ Each department will be audited periodically for compliance.



## Records & Information Management

### SCOPE AND OBJECTIVES

- ◆ Identify and Secure Vital Records.
- ◆ Institute a Disaster Recovery Plan for all company records and information.
- ◆ Ensure legal compliance and audit protection.
- ◆ Minimize litigation risks.
- ◆ Assimilate new records management technologies.
- ◆ Access to valuable information and costs saving.

## A RECORD IS...

A record is any or all recorded information, regardless of medium or specific characteristics, created, received, used or distributed by MCI in the course of its business. This includes paper, microfilm, tape, microfiche, e-mail, PC hard drives, mainframes, mid-range systems, voice mail, optical, intranet and other mediums.



Only the *official copyholder* of a record is required to retain a record for the total retention period indicated in the RRS. If you maintain originals, you are the official copyholder. Creating a record does not mean you are the official copyholder; you must also maintain the original. Copies should not be stored or kept once your operational need is completed.

Drafts documents should not be retained once a document is finalized. Drafts have no retention requirement and must not be retained in any media form. However, it is acceptable to hold drafts until a document is finalized, then they should be purged.



## E-MAIL

E-mail is just another form in which records/information is received.

- ◆ E-mail received or created in the course of business is an official record. It is the message within the e-mail that should be considered for retention, not who the message is from.
- ◆ The retention period is based on the content of the message. For example, an e-mail message between a MCI employee and a vendor must be retained for the time period specified for vendor correspondence.
- ◆ Keep in mind that, approximately, one percent or less of all e-mail sent or received has a true retention value. For internal e-mail messages, the sender has the obligation to follow any retention requirements, not the recipients. For e-mail messages coming from an external source, the recipient needs to either purge or retain pursuant to the Records Retention Schedule. Since a majority of e-mail has no retention requirement, all employees should be deleting e-mail once the retention requirement or operational need is complete. Operational need should not exceed one year from the receipt or sending the message.
- ◆ Specific company policy on e-mail, as written by Legal, can be located at: <https://teamnet2.mcilink.com/departments/lppgc/techlaw/>

## **VITAL RECORDS**

- ◆ Vital records contain information that is essential to reestablishing or continuing an organization in the event of a disaster.
- ◆ Vital records are essential:
  - to continue Company operations,
  - to recreate the Company's legal and financial position, and
  - to preserve the rights of the Company, its employees, customers, and stockholders.
- ◆ Examples of Vital Records are: ledgers & journals, customer billings, mergers, articles of incorporation, patents/copyrights and stockholders registers, design/documentation.

## **DISASTER RECOVERY PLAN**

Used in the salvaging of records of various media types (paper, CDs, diskette, tape, electronic, etc.) when disaster strikes.

- ◆ Focus of the plan is designed to:
  - minimize disruption of normal business operations
  - prevent further escalation of the disruption
  - minimize the economic impact of the disaster
  - establish alternative operating procedures
  - recover/salvage organizational assets
  - provide for rapid and smooth
  - train personnel with emergency procedures
- ◆ Each department responsible for Vital Records must have a Disaster Recovery Plan.
- ◆ The Plan must be provided to Records and Information Management.



## WANT TO IMAGE YOUR RECORDS? ALREADY DOING SO?

- ◆ Is imaging a cost effective way to handle your records versus using off-site storage? If using off-site storage, you can have your records within 2 hours.
- ◆ Imaging systems should be used for day-to-day use and the need of quick retrieval, not for long-term storage.
- ◆ Originals of imaged documents need to be retained if the retention period is longer than 5 years; however, you must get written approval from RIM, Legal and Tax to destroy the originals after they have been imaged.
- ◆ If initiating an imaging system with your department, there may be IRS regulations or legal criteria that should be followed. RIM or the Tax department can provide a copy of the revenue procedures.
- ◆ A binder with the following data must be created and maintained on-site:
  1. A record of what you are imaging, where, when, and on what equipment any document was imaged will be maintained (to be retained in history format).
  2. An accurate chronological record of changes to the system. This must be maintained for as long as the system is running.
  3. Evidence of procedures ensuring quality, reliability and the integrity of the documents being imaged, including audit procedures.
  4. A list of MCI management personnel responsible for the supervision of the system (systems and record imaging). Provide names, dates, and titles. This needs to be updated when the "players" change.
  5. Documentation on the initial system, and any significant change to the system. Any major changes need to be discussed with the Tax department.
  6. A description of the optical platters used for storage, and location of where back-up copies will be maintained.
  7. Identify the location of records that are not or cannot be imaged.
  8. Procedures for retrieving records from imaging system.

## MANAGER RESPONSIBILITIES

- ◆ All Managers' working files for employees should be sent to the HR Fileroom once an employee no longer works for the company or your department. If an employee transfers to another department, you should send any manager notes regarding the employee to the HR Fileroom. It is acceptable, however, to give the new manager the employee's attendance record, performance review and PAF, but you cannot give those notes or written comments that are about or concern the employee.
- The HR Fileroom is located at: 9835/700, 707 17th Street, Denver, Colorado 80202
- ◆ When an employee leaves the company, all files on his/her computer must be reviewed (including e-mail and e-mail attachments) for retention requirements under the Records Retention Schedule. The computer's records should be either retained or destroyed. Files that require retention must be pulled off the computer and stored appropriately. After this review, the computer's hard drive must be wiped clean of all records before being issued to a new user (even if this new user is in the same department).
- ◆ If a Manager receives a request from a terminated employee regarding getting copies of their travel and expense records or records contained within their personnel file, the Manager must refer the terminated employee to Law & Public Policy (LPP). No records or information may be given out to terminated employees (voluntary or involuntary) without prior approval from LPP.

# RECORDS RETENTION SCHEDULE

## (RRS)

- ◆ A tool that identifies those records requiring retention and their required retention period.
- ◆ The retention periods in the RRS are based on federal, state or local regulations and the company's operational needs.
- ◆ Retaining records longer than their legal or operational requirement exposes MCI to unnecessary financial and legal risk.
- ◆ MCI must avoid the perception that we are selectively disposing of records.
- ◆ Primary objective is for prompt disposal of records whose retention period has been met.
- ◆ Based on the company's functional areas and records common to those areas.
- ◆ Assigns each "type" of record its unique Record Series (RS) number. Determination, by the user, of the correct RS number is important in calculating the correct destruction review date.
- ◆ "Just in case" is not a consideration in retention. Individual departmental determinations do not supersede or replace the MCI Record Retention Schedule. Requested exceptions are submitted to RIM.



**Record Retention**

## RECORDS MANAGEMENT COMPLIANCE AUDIT

### Some factors for compliance:

- ◆ Are all employees aware of and in compliance with the retention program?
- ◆ Does the department recognize what a record is?
- ◆ Is the department reviewing and retaining their records, on-site & off-site, in accordance with the Record Retention Schedule?
- ◆ Is your department storing their records off-site properly?
- ◆ Can records be retrieved in a timely and efficient manner (off-site and on-site)?
- ◆ Does your department recognize that e-mail and anything downloaded from the internet are records?
- ◆ Is your department deleting e-mail and electronic data when operational need or legal retention requirements are surpassed?
- ◆ Does your department handle Vital Records?
- ◆ Does your department have a Disaster Recovery Plan?

If you want to make sure that your department is compliant with the Records Management Program before a formal audit is conducted, please call RIM.

## OFF-SITE STORAGE



Off-Site

- ◆ All procedures associated with off-site storage are detailed on RIM's website.
- ◆ What you put into storage is your individual responsibility. If someone tells you to send something to storage (or retain it on-site) and you know it is against retention policy, you must challenge that request.
- ◆ All costs are paid by the RIM department, with the exception of:
  - Cartons returned to the submitter because of absence of inventory data.
  - Non-response to service request. You requested service from the storage vendor, but both you and your designated alternate point of contact were not present when the vendor's 'driver' arrived to deliver/pickup.
  - Rush orders.
- ◆ Any questions or problems that you have about off-site storage, contact RIM. Do not contact the storage vendor.
- ◆ Review the records you are planning to archive to ensure they have a retention requirement. Only those records should be placed in off-site storage.
  - No copies, working papers, drafts, miscellaneous manuals, stuff from past employee's office/desk (w/o review), no data in electronic form unless the associated software/hardware system is retained.
- ◆ Standard Storage & Climate-Control Storage.
  - Climate controlled storage is available for records retained on such media as microfiche, CD, tape, etc. You must indicate this type of storage to the vendor (on the MCI Inventory Form) when submitting the materials to storage.
- ◆ Only 'like' records can be put in to each storage carton.
  - Invoices separated from correspondence. They have different RS codes – have different retention requirements.

## **OFF-SITE STORAGE**

### **continued**

♦ **Completion of the MCI Inventory Form:**

- Use only the MCI Inventory Form (or the MCI Master Inventory Form), which can be downloaded from RIM's website.
- The storage vendor will refuse pick up if inventory forms are not with the cartons. With no exceptions.
- Complete every entry on the Inventory Form, except for the Retention Code.
- If entries are not completed correctly or clearly, retrieval of records will be very difficult and the proper retention period of the records may be jeopardized.
- Research the Record Classification Code (RS#) within the Record Retention Schedule. If you need any assistance, please contact RIM. It is imperative that you assign the correct RS# to ensure proper retention.
- Use a clear description; a description recognizable by anyone in the company. Do not use acronyms, the words – miscellaneous, completed, JJ Bean's desk, inactive records, etc.
- Complete the electronic request form, located on RIM's website, for pick-up of new storage. This form is directly e-mailed to RIM. In addition, you must fax a copy of your Inventory Form(s) to RIM for review. We will review the forms for completeness and clarity, to avoid problems in the future. Once the inventory form has been approved, RIM will forward your request for new storage pick-up to the storage vendor.
- Xerox a copy of the Inventory Form for your records. Put the original with the cartons for pick up.
- Do not complete Inventory Forms for someone else; for example, someone directs you to 'send these files to storage' – but they are records that you have never worked. It is the responsibility of the employee that maintains the records, to review those records and prepare the Inventory Form. If RIM, or LPP or Tax, needs to inquire about inventory data on records, we must speak to the individual with knowledge about the records.

## **OFF-SITE STORAGE**

### **Continued**

- ◆ Requests for retrieval and refile are done through RIM's website and transmitted directly to the storage vendor. Requests for new storage pick-up or supplies are transmitted to RIM via the request forms on RIM's website. Once new storage or supply orders have been reviewed and approved, RIM will forward the request to the storage vendor. The storage vendor will respond with a confirmation email, providing their delivery/pick-up date and a service order number.
- ◆ The vendor provides next-day service, if your order is received before 4pm.
- ◆ Following are the service requests available:
  - “*Storage Supply Requests*”: Storage supplies to include boxes and barcode labels. The Inventory Form requires a barcode number for each carton and a corresponding larger barcode label is affixed to the side of each carton. (only 1.2 cubic ft cartons are used. Contact RIM for exceptions.)
  - “*Electronic Box Retrieval Request Form*”: To request retrieval of a box from storage.
    - “*Electronic New Storage Pickup Form*”: To pick-up cartons that need to go to storage that have never been to storage.
    - “*Electronic Box Refile Form*”: To pick-up cartons previously retrieved from the storage vendor.
  - The “*HR File Request/Return Form*” is utilized only by the HR fileroom in Denver.
    - “*File Level Request/Return Form*”. This is used to request individual files from a carton. This can only be done if all of the files contained in the carton have been individually inventoried and identified, which would assign each file its own file id# in addition to the carton’s barcode number. For further information on file-level inventory, contact RIM.

## **OFF-SITE STORAGE**

### **Continued**

◆ Other points.....

- When completing the request form on the website, make sure you indicate the “District” in the pull-down menu.
- You must provide a dept# (or an 8-digit dept name/abbrev)
- You must provide an “Alternate Contact Name” (point of contact). This is for the vendor’s driver. Make sure you tell your ‘alternate’ what service you requested, where the cartons are or what is expected to be delivered, and that the inventory forms are with the cartons.
- Do not contact the storage vendor via telephone or by any other means besides your service requests.
- MCI records will not be delivered to mailrooms or left on delivery docks under any circumstances. The storage vendor has been notified of this policy. Contact RIM for exceptions, to include strong justification.
- Cartons retrieved from storage may only be ‘outcarded’ for ten business days. RIM will notify you to return the carton(s) after this period or submit a justification to extend the retrieval time.

MCIWC031911



## **YOU MUST CONTACT RIM IF...**

- ◆ You are storing active records.
- ◆ You need to retrieve records from off-site and reactivate them as active records on-site.
- ◆ If you are consolidating cartons of records stored off-site. The barcode numbers must be accounted for.
- ◆ If you have records stored off-site that have been identified for an audit or to be held due to a litigation. A retention hold code will be assigned to the carton.
- ◆ If you need to retain records retrieved from storage longer than 10 business days.
- ◆ If you have special requests regarding off-site storage.
- ◆ If you have questions or difficulties with services provided by the storage vendor or RIM.
- ◆ If you have questions regarding records, what type of media to use for storing records, you are moving to another location, the department is closed, or you find records stored in a self-storage facility or somewhere other than the office or Iron Mountain.